Lutte contre le terrorisme: traitement et protection des données personnelles dans le cadre de la coopération policière et judiciaire en matière pénale. Décision-cadre

2005/0202(CNS) - 07/06/2007 - Texte adopté du Parlement après reconsultation

Le Parlement européen a adopté le rapport de **Martine ROURE** (PES, FR) modifiant, dans le cadre de la procédure de consultation, la proposition de décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale. Le Parlement était reconsulté sur cette proposition qui avait déjà fait l'objet d'un avis du Parlement en juin 2006 (se reporter au résumé daté du 14/06/2006).

Les principaux amendements du Parlement sont les suivants :

- champ d'application : les députés estiment que la décision-cadre doit s'appliquer à l'ensemble des autorités nationales, sans exception. Aussi ont-ils supprimé une disposition qui aurait exclu « les autorités ou autres organismes qui traitent des questions de sécurité nationale ». Ils ont également introduit une nouvelle disposition invitant la Commission à soumettre, au plus tard trois ans après la date d'entrée en vigueur de la décision-cadre, des propositions en vue d'élargir son champ d'application au traitement des données à caractère personnel dans le cadre de la coopération policière et judiciaire au niveau national ;

- licéité du traitement des données personnelles : selon les députés, les données à caractère personnel doivent être évaluées en tenant compte de leur degré d'exactitude ou de fiabilité, de leur source, des catégories de personnes concernées, des fins auxquelles elles sont traitées et de la phase au cours de laquelle elles sont utilisées. Les données inexactes ou incomplètes doivent être effacées ou rectifiées. L'exploration de données et toute forme de traitement à grande échelle de quantités massives de données, en particulier lorsqu'elles se rapportent à des personnes non suspectes, y compris le transfert de ces données à un autre responsable du traitement, ne sont autorisés que dans certaines circonstances. Les données doivent être traitées en séparant les faits et les évaluations objectives des avis ou des évaluations personnelles, et en séparant les données relatives à la prévention et à la poursuite des infractions des données détenues licitement à des fins administratives. Les données qui sont mises à disposition des autorités compétentes des autres États membres doivent être régulièrement vérifiées et mises à jour pour garantir un accès à des données exactes;

- pour les députés, le traitement des données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle, est par principe interdit, et ne peut être toléré qu'en cas d'absolue nécessité et dans un cadre légal clair ;

- les données qui ont été transmises ou mises à disposition par l'autorité compétente d'un autre État membre ne peuvent être traitées ultérieurement, pour des finalités autres que celles pour lesquelles elles ont été transmises que sous réserve des dispositions législatives nationales et uniquement « pour toute autre finalité déterminée, légitime et non excessive par rapport aux finalités pour lesquelles elles sont enregistrées » ;

- **transfert de données aux pays tiers** : les députés estiment que la décision-cadre ne doit pas avoir pour conséquence une réduction du niveau de protection qui résulterait de dispositions nationales ou de

conventions internationales. Le texte stipule que le transfert de données à des pays tiers ou à des instances ou organisations internationales ne peut de manière générale être toléré que si ce transfert est nécessaire pour la prévention, la recherche, la détection ou la poursuite des infractions terroristes et d'autres infractions pénales graves, si l'État membre duquel les données ont été obtenues a donné son accord au transfert conformément à son droit national et si le pays tiers ou l'instance internationale concerné assure un niveau de protection adéquat pour les données considérées. À titre exceptionnel, les données peuvent être transférées aux autorités compétentes de pays tiers ou à des instances internationales n'assurant pas un niveau adéquat de protection, en cas d'absolue nécessité afin de sauvegarder les intérêts essentiels d'un État membre, ou à des fins de prévention de menaces imminentes graves à l'encontre de la sécurité publique ou d'une ou de plusieurs personnes en particulier ;

- **transmission à des autorités autres que les autorités compétentes** : les données ne peuvent être transmises à des autorités d'un État membre autres que les autorités compétentes que dans des cas particuliers individuels et dûment justifiés et si certaines conditions sont réunies ;

- **transmission à des personnes privées** : les États membres doivent veiller à ce que les données ne soient transmises à des personnes privées dans un État membre que dans des cas particuliers et si certaines conditions sont réunies. En particulier, la transmission doit faire l'objet d'une obligation ou d'une autorisation légale claire. Les autorités compétentes pourront consulter et traiter les données contrôlées par des personnes privées uniquement au cas par cas, dans des circonstances spécifiques, pour des motifs spécifiques et sous contrôle judiciaire au sein des États membres. De plus, lorsque les personnes privées collectent et traitent les données dans le cadre d'une mission de service public, elles doivent être soumises à des obligations au moins équivalentes ou supérieures à celles imposées aux autorités compétentes ;

- **l'autorité de contrôle commune** devrait regrouper les autorités de contrôle nationales et le contrôleur européen de la protection des données ;

- **évaluation et révision** : trois ans au plus tard après la date d'entrée en vigueur de la décision cadre, la Commission présentera au Parlement européen et au Conseil une évaluation de l'application de la décision-cadre assortie de propositions de modification qui seraient nécessaires afin d'élargir le champ d'application.

Le Parlement a également ajouté les **15 principes généraux** proposés par la Commission en annexe, afin qu'ils fassent l'objet d'une prise de position formelle de la part de toutes les institutions. Ces principes sont, entre autres, la protection des droits et libertés, la transparence, la légitimité et la proportionnalité du traitement, la qualité des données, les droits d'information et de rectification, la confidentialité et la sécurité, ou encore la responsabilité et les possibilités de recours.

Selon les députés, la décision-cadre n'est que la première étape vers la définition d'un cadre plus global et cohérent de la protection des données à caractère personnel utilisées à des fins de sécurité. Un tel cadre peut s'inspirer des principes annexés à la décision-cadre.